UNTRUSTED MOBILE APPLICATIONS

STATE OF ART OF SECURITY APP-APOCALYPSE

YURY CHEMERKIN

MULTI-SKILLED SECURITY EXPERT

[AGENDA]

- ~~Intro~~
- First Part “What we already know about insecurity?”
- Second part “What are we going to know?”
- Third Part “What we can do with that?”
- Conclusion

[AGENDA]

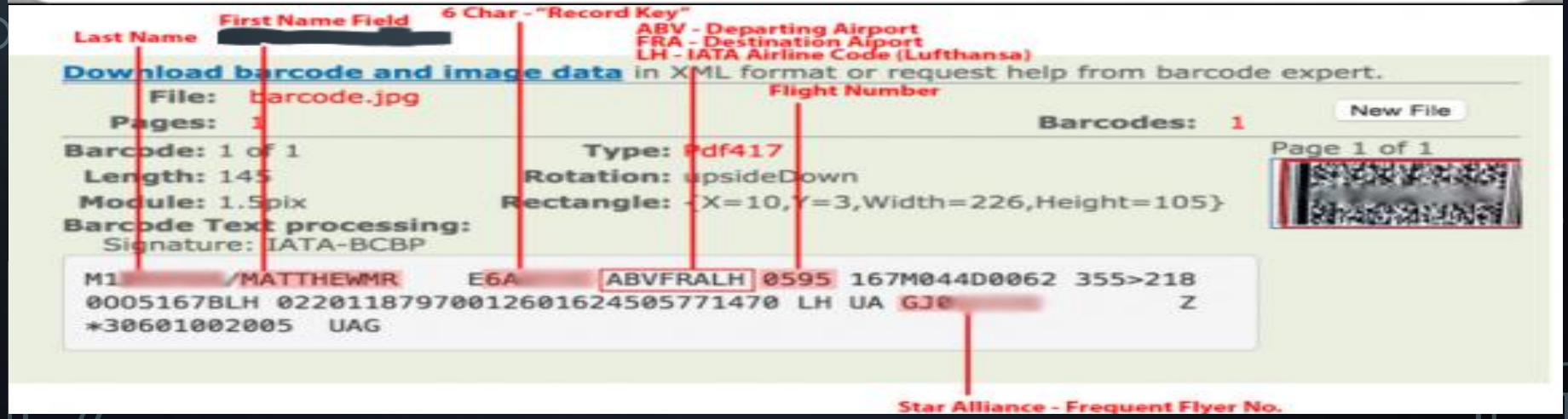
- ~~Intro~~

1. **First Part "What we already know about insecurity?"**
   - **InSecurity & InPrivacy Problem**
   - Poll
   - Quotes about insecurity from researchers and
   - What companies think about 'quotes'
   - Facts about app insecurity
   - How can you make your app fail

PROBLEM. WHAT/WHO MAKES US INSECURE?

- Are we revealing everything about ourselves everywhere?
  - Perhaps
- Don't we know anything about security and privacy?
  - Perhaps
- Aren't app developers responsible for security fails?
  - Who said they're not? They are!
  - They prefer not to tell about it only

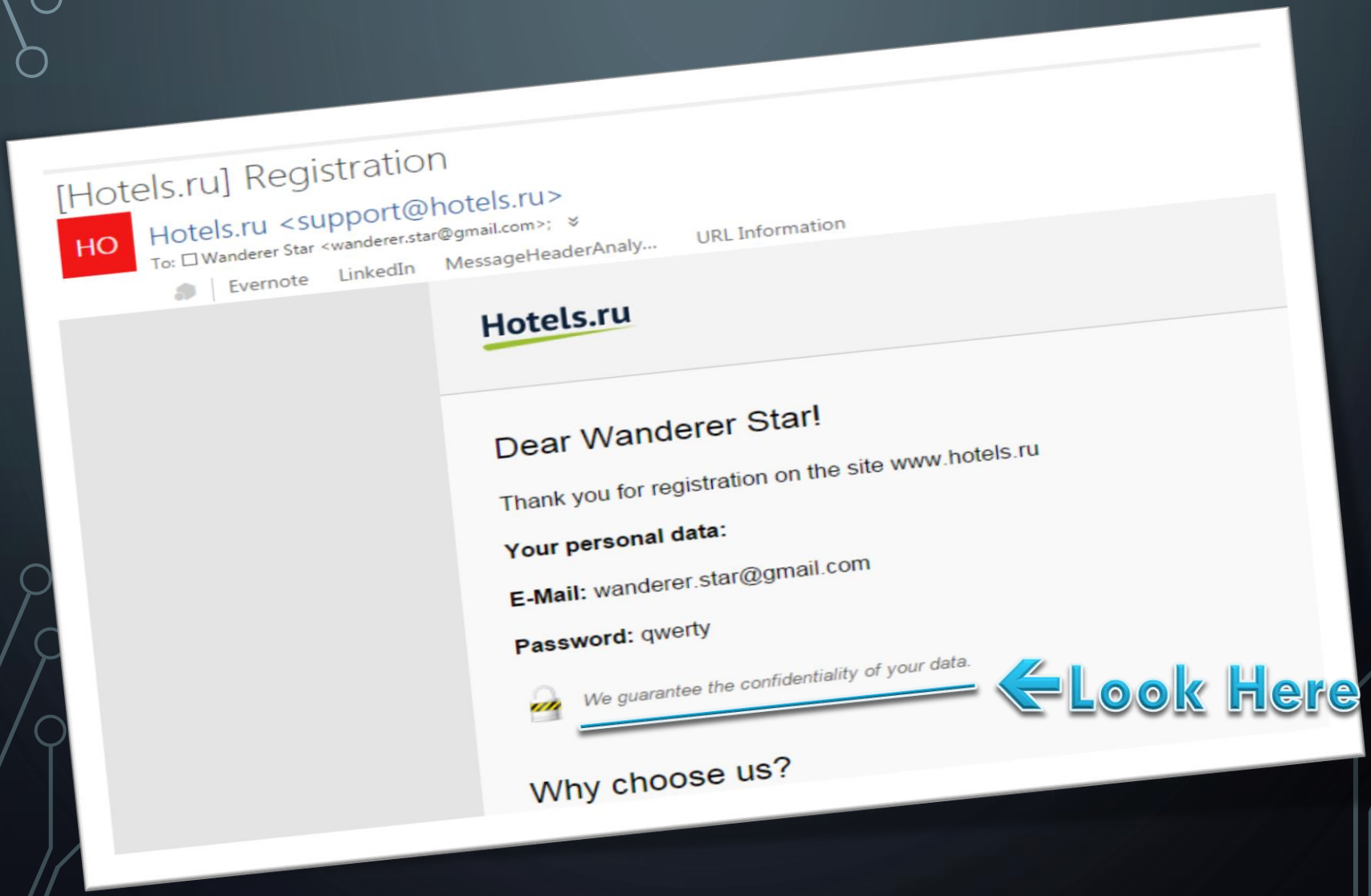
HONESTLY, THIS IS OLD STORY BUT… ONE MONTH AGO…[Y2015]



HONESTLY, THIS IS OLD STORY BUT… ONE MONTH AGO…[Y2015]

- The news is sure to be a blow to jet-setters all over the internet, as sites like Instagram and Facebook are rife with boastful photos of boarding passes to exotic locales.
- "The next time you're thinking of throwing away a used boarding pass with a barcode on it, consider tossing the boarding pass into a document shredder instead.
- "Besides his name, frequent flyer number and other [personally identifiable information], I was able to get his record locator (a.k.a. "record key" for the Lufthansa flight he was taking that day," Cory said. "I then proceeded to Lufthansa's website and using his last name (which was encoded in the barcode) and the record locator was able to get access to his entire account. Not only could I see this one flight, but I could see ANY future flights that were booked to his frequent flyer number from the Star Alliance."
    - http://krebsonsecurity.com/2015/10/whats-in-a-boarding-pass-barcode-a-lot

WE GUARANTEE THE CONFIDENTIALITY OF YOUR DATA



WE GUARANTEE THE CONFIDENTIALITY OF YOUR DATA

- Confidentiality - In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes" (Excerpt ISO27000).

- https://en.wikipedia.org/wiki/Information_security#Confidentiality

HOW MUCH DOES YOUR SECURITY COST?

- Non-Special ‘Home’ Software

  - Macroplant Software - $35-70 (home), $200-2500 (enterprise).

  - XK72 Software - $50 per license or $400-700 per bundle
  - PortSwigger - $300 per year

  - … and so on

  - *Also, cracked edition is available (no difference pirate or buy ☺)*

- Special ‘Forensics’ Software

  - Elcomsoft Breakers - $80 (home, you have to know your password), $200 (pro – you don’t have to know it), $800 – bundle

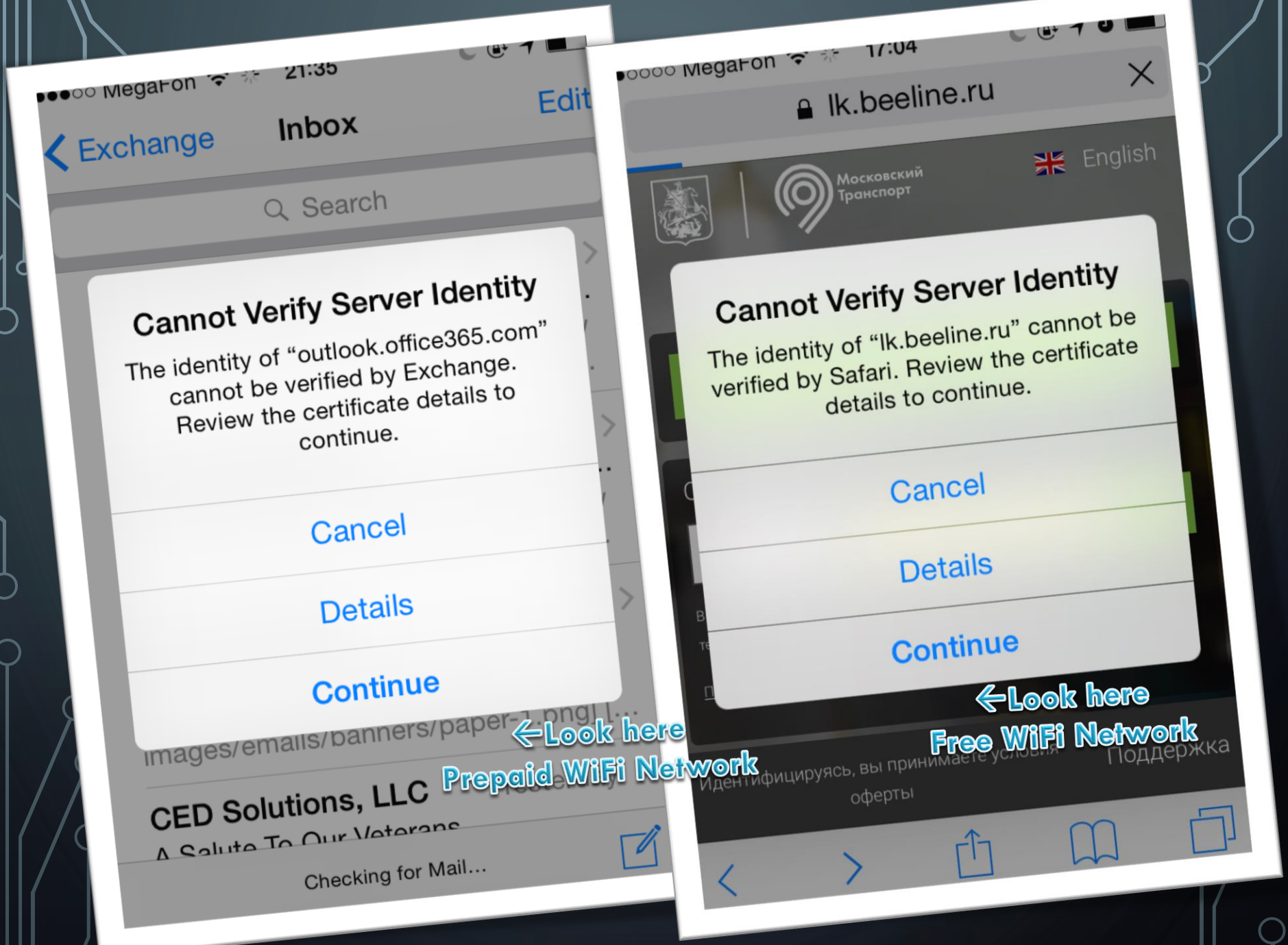
  - Elcomsoft Bundles - $1 500 – 2 500

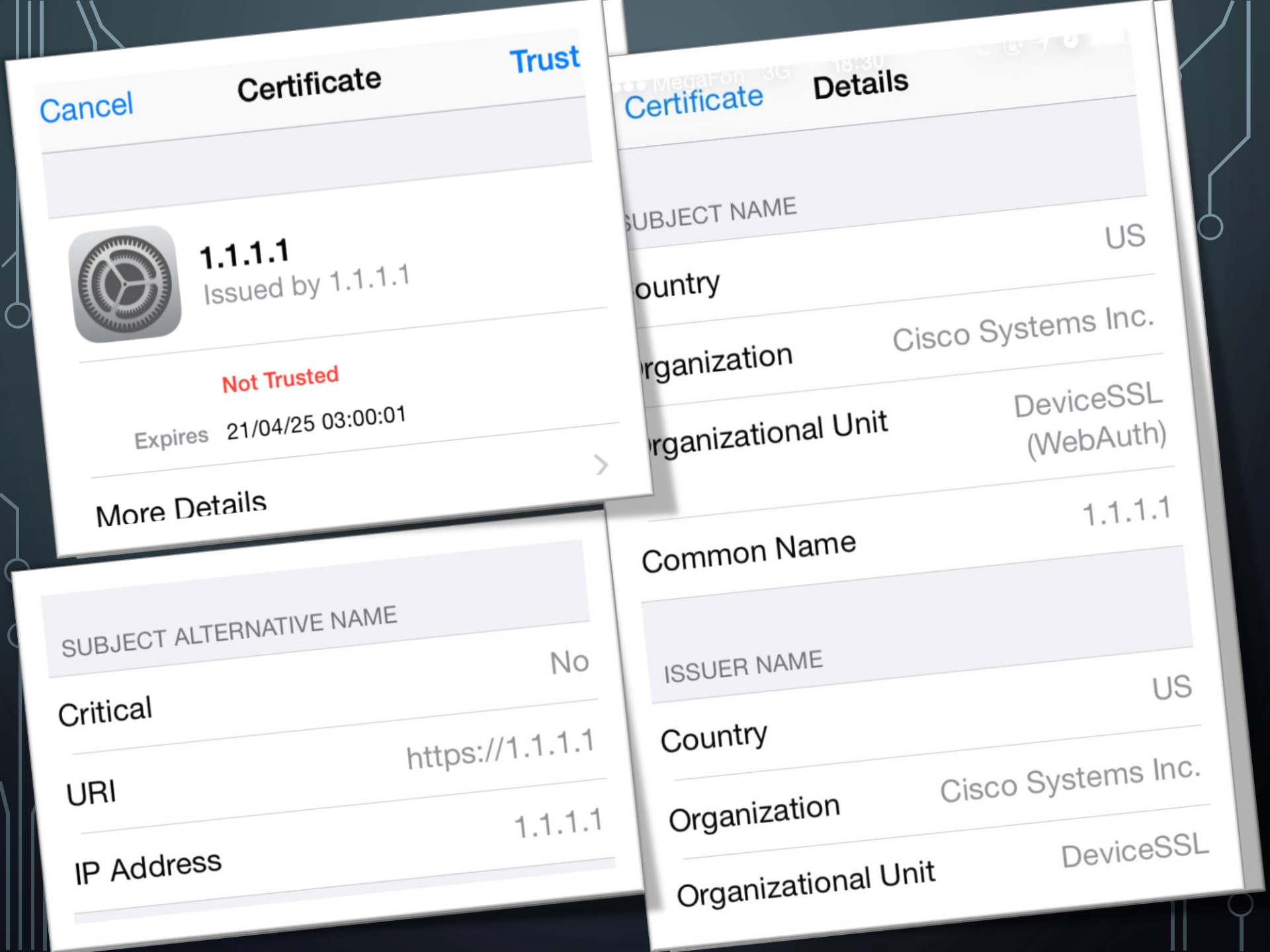
  - Oxygen Software – more expensive in twice at least
  - … and so on

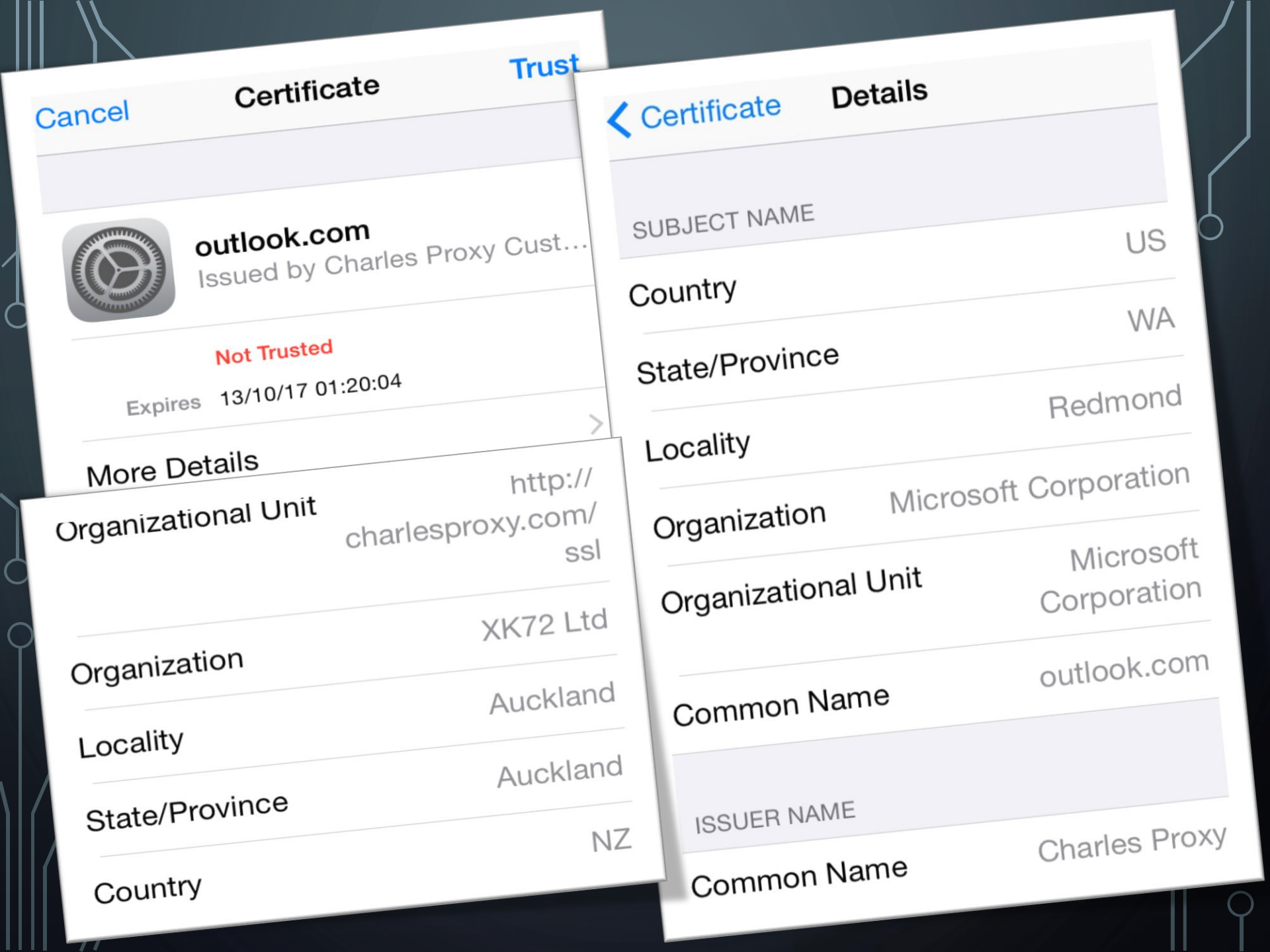
  - *Also, cracked edition is available for some old editions (better buy new edition ☺)*

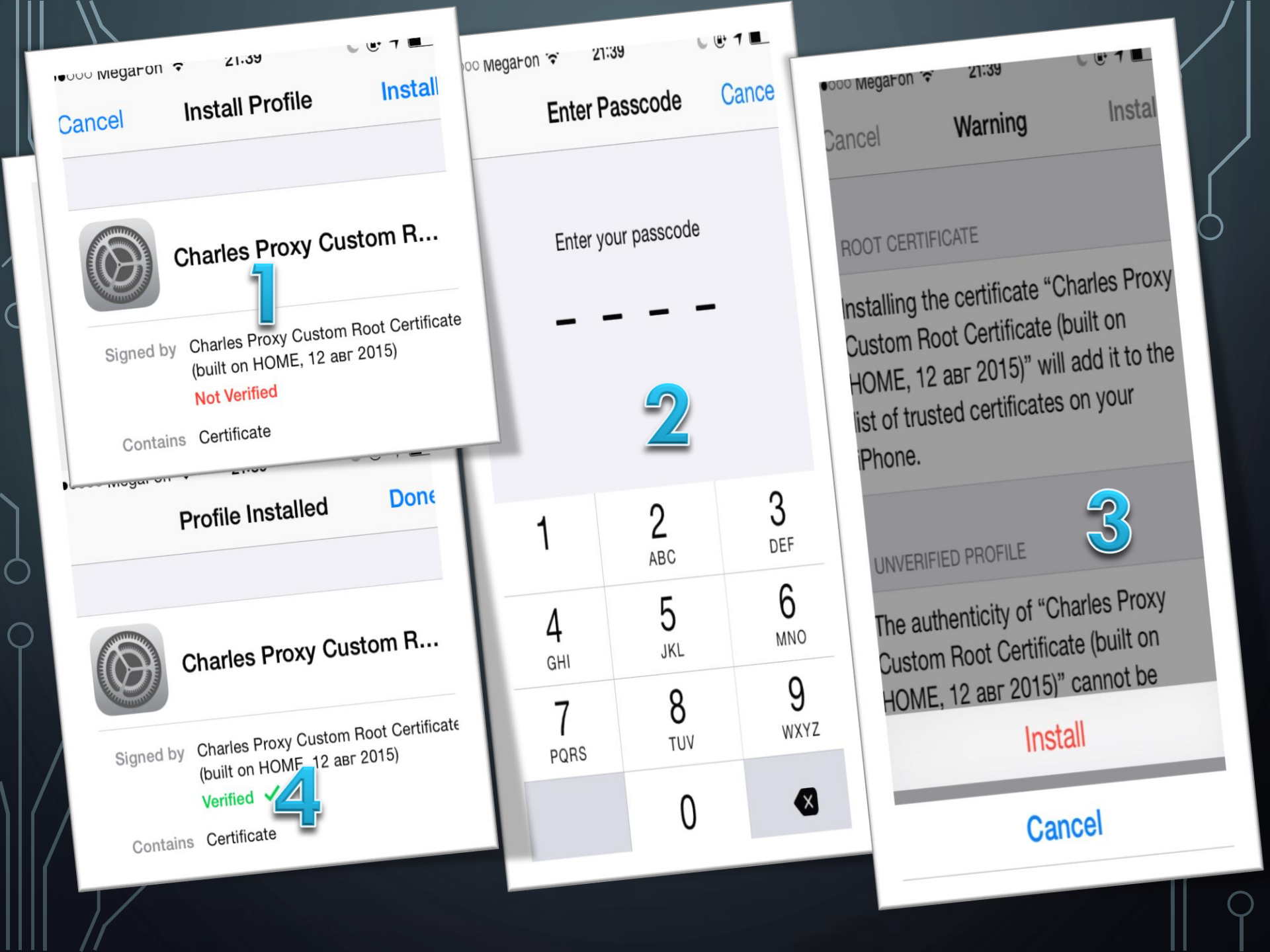
UNTRUSTED PLACES

- Untrusted chargeable places.
  - When you connect your device to them you will see a notification you plugged to PC/Mac
- Untrusted network places.
  - When you connect your device to them
    - You will see nothing
    - You will see a question about untrusted certificate. You accept or decline it
    - Someone make you to install trusted certificate

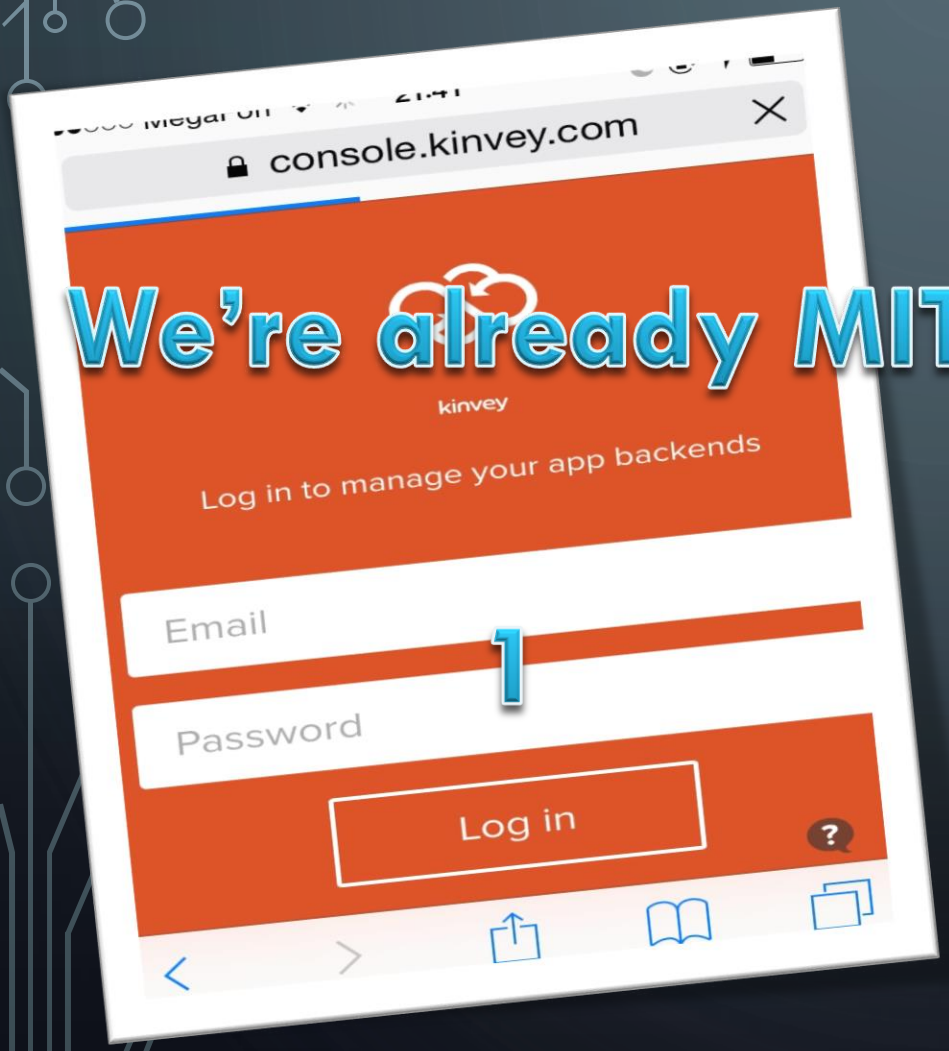

MegaFon 21:35
Exchange
Inbox
Edit
Search
Cannot Verify Server Identity
The identity of “outlook.office365.com” cannot be verified by Exchange. Review the certificate details to continue.
Cancel
Details
Continue
images/emails/banners/paper-1.png
CED Solutions, LLC
A Salute To Our Veterans
Checking for Mail…
←Look here
Prepaid WiFi Network
MegaFon 17:04
lk.beeline.ru
English
Московский Транспорт
Cannot Verify Server Identity
The identity of “lk.beeline.ru” cannot be verified by Safari. Review the certificate details to continue.
Cancel
Details
Continue
←Look here
Free WiFi Network
Идентифицируясь, вы принимаете условия
оферты
Поддержка


Cancel
Certificate
Trust
1.1.1.1
Issued by 1.1.1.1
Not Trusted
Expires 21/04/25 03:00:01
More Details
SUBJECT ALTERNATIVE NAME
Critical No
URI https://1.1.1.1
IP Address 1.1.1.1
Certificate
Details
SUBJECT NAME
ountry US
rganization Cisco Systems Inc.
rganizational Unit DeviceSSL (WebAuth)
Common Name 1.1.1.1
ISSUER NAME
Country US
Organization Cisco Systems Inc.
Organizational Unit DeviceSSL


Cancel
Certificate
Trust
outlook.com
Issued by Charles Proxy Cust…
Not Trusted
Expires 13/10/17 01:20:04
More Details
Organizational Unit http://charlesproxy.com/ssl
Organization XK72 Ltd
Locality Auckland
State/Province Auckland
Country NZ
Certificate
Details
SUBJECT NAME
Country US
State/Province WA
Locality Redmond
Organization Microsoft Corporation
Organizational Unit Microsoft Corporation
Common Name outlook.com
ISSUER NAME
Common Name Charles Proxy

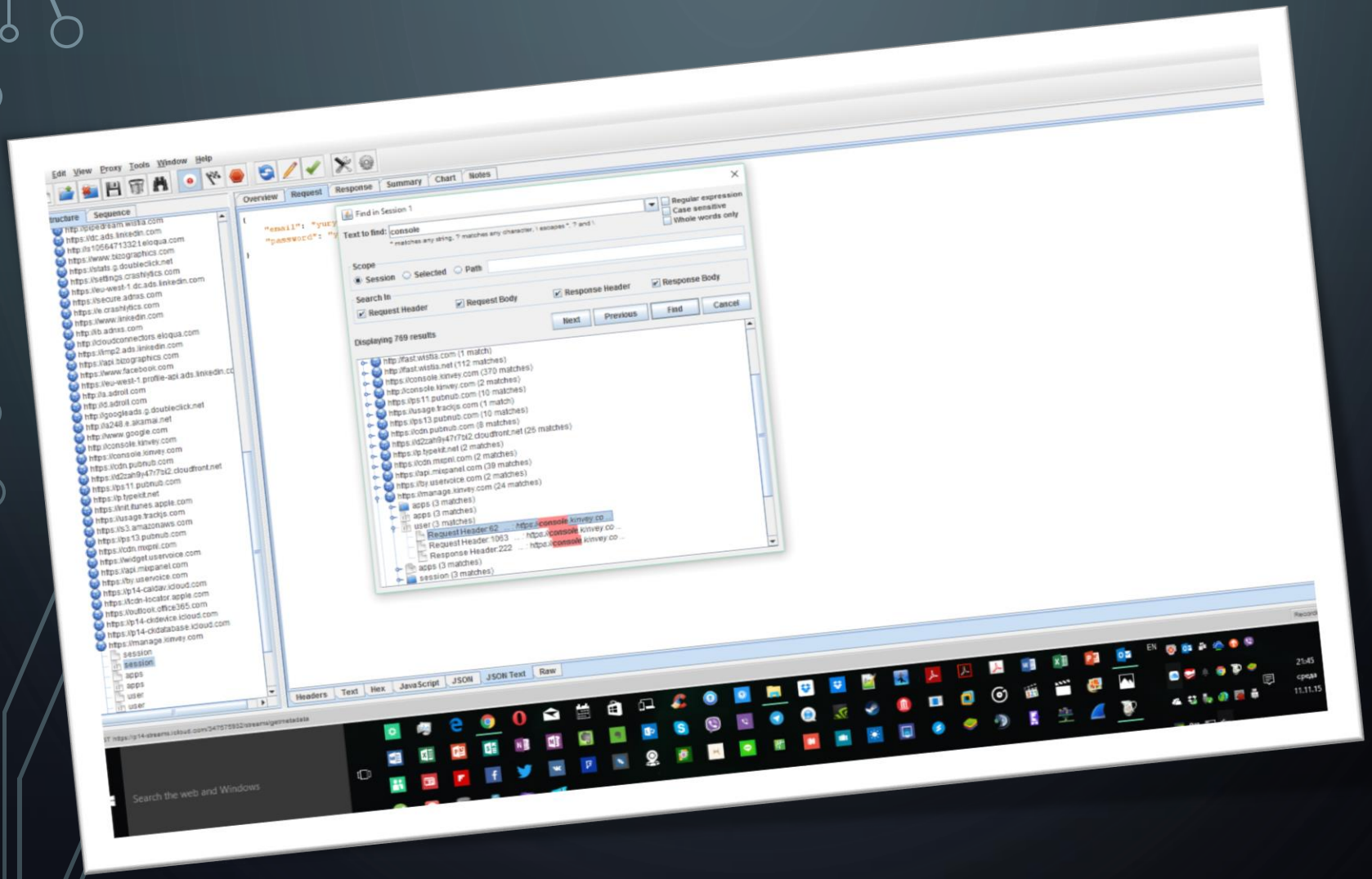

Cancel
Install Profile
Install
Charles Proxy Custom R...
1
Signed by Charles Proxy Custom Root Certificate (built on HOME, 12 авг 2015)
Not Verified
Contains Certificate
Profile Installed
Done
Charles Proxy Custom R...
Signed by Charles Proxy Custom Root Certificate (built on HOME, 12 авг 2015)
Verified
4
Contains Certificate
Enter Passcode
Cance
Enter your passcode
2
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
Cancel
Warning
Instal
ROOT CERTIFICATE
Installing the certificate “Charles Proxy Custom Root Certificate (built on HOME, 12 авг 2015)” will add it to the list of trusted certificates on your iPhone.
UNVERIFIED PROFILE
3
The authenticity of “Charles Proxy Custom Root Certificate (built on HOME, 12 авг 2015)” cannot be
Install
Cancel

UNTRUSTED PLACES.
KINVEY IS A BACKEND FOR STORING FILES & USER ACCOUNTS

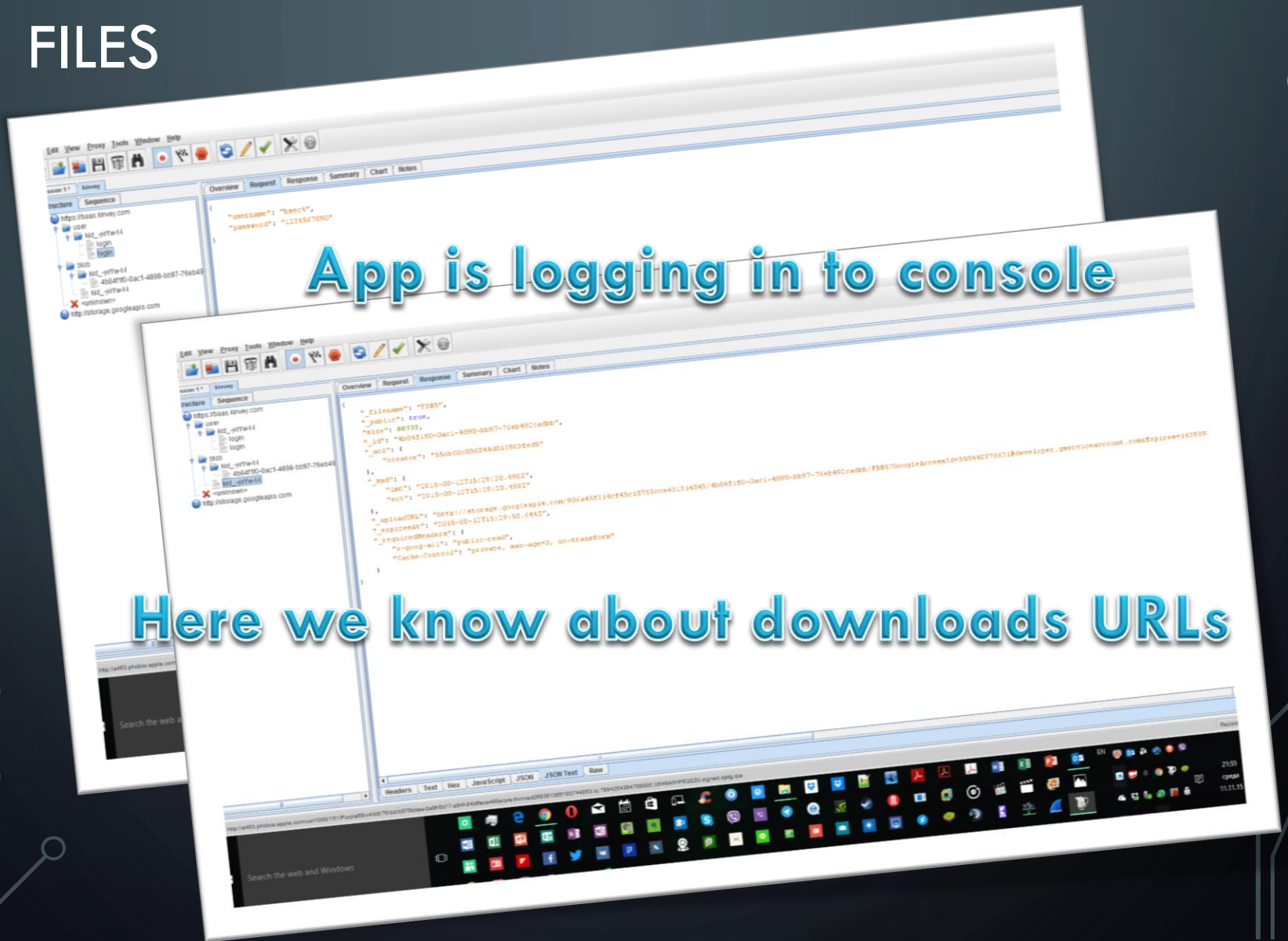


We're already MITMing the network

UNTRUSTED PLACES. KINVEY.
ADMIN IS LOGGING IN TO KINVEY CONSOLE



UNTRUSTED PLACES. KINVEY. APP IS LOGGING IN & DOWNLOADING FILES



[AGENDA]

- ~~Intro~~

1. **First Part "What we already know about insecurity?"**
   - ~~InSecurity & InPrivacy Problem~~
   - **Poll**
   - Quotes about insecurity from researchers and
   - What companies think about 'quotes'
   - Facts about app insecurity
   - How can you make your app fail


GONNA MAKE THEM A POLL
GEEKS LOVE POLLS

HTTPS://GOO.GL/ABZJ1P

- Tell what is data protection to you?

[AGENDA]

- ~~Intro~~

1. **First Part "What we already know about insecurity?"**
   - ~~InSecurity & InPrivacy Problem~~
   - ~~Poll~~
   - **Quotes about insecurity from researchers**
   - What companies think about 'quotes'
   - Facts about app insecurity
   - How can you make your app fail

WHAT DO RESEARCHERS TALK ABOUT APP DATA INSECURITY?

- Guys, are you really sending my pass to 'iphone-xml.booking.com' w/o MITM protection if I'm on Android Emulator even?
  - Booking.Com (Hotel App)
- What are you storing my login, password and auth token in the same place for?
  - Many apps lke ICQ (IM Messenger App)
- Wtf guys, you don't have any network protection for my credentials? An access to mail credentials gives everything!
  - Many mail & other apps like Mail.Ru Mail (Mail App)
- I got access to emails. Why if I already had access to credentials?
  - Many mail apps like Mail.Ru Mail (Mail App)

WHAT DO RESEARCHERS TALK ABOUT APP DATA INSECURITY?

- I feel like this app re-download all my attachments to somewhere
  - MS Outlook App (Mail App), server for attachment is [files.acompli.net]
- App #1. Here, I see my credentials for App #2. Same vendor. Why did you duplicate my credentials everywhere?
  - Word, Excel, PowerPoint – App#1, OneDrive – App#2 (Office Apps)
- You had no right to take my IMEI! I will… wait I'm on Android Emulator, no worries it's fake IMEI !
  - RSB (Bank App)
- Unique user ID in each request and same in response. Let's put fake ID in request? We bruteforced all users ID and their customer buckets!
  - <…> (School eLearning Paid App)

[AGENDA]

- ~~Intro~~

1. **First Part "What we already know about insecurity?"**
   - ~~InSecurity & InPrivacy Problem~~
   - ~~Poll~~
   - ~~Quotes about insecurity from researchers~~
   - **What companies think about 'quotes'**
   - Facts about app insecurity
   - How can you make your app fail

WHAT COMPANIES THINK ABOUT ‘QUOTES’ AND INSECURITY

- Instagram said it's moving to encrypted communications for its images by moving to HTTPS, the secure version of the standard used to transfer Web data over the Internet.
  - They did it but it’s still affected to MITM attacks

- "Message data is stored in an unencrypted format because the operating systems (both iOS and Android) provide data isolation that prevents apps from having their storage read by other apps. This is considered standard in the industry, and is completely safe," the Kik said.
  - Standard… it’s safe… just ROFL… and did you know there is way to root device without owner knowledge?

WHAT COMPANIES THINK ABOUT ‘QUOTES’ AND INSECURITY

- SECURITY is core at 4Talk. Starting from secure phone number registration, to interaction only with confirmed personal contacts, to fully managing your account from any device you use.
  - Y2014 wasn’t protected at all
  - Y2015: Protected for Windows in-rest & transit, prevent MITM
  - Y2015: Protected for Android in-transit only, prevent MITM
  - Y2015: Not protected for iOS and Mac OS at all
- Data Leakage is data that becomes available when you perform typical activities. Instead, Vulnerability is a weakness of program. Thus, Vulnerability ≠ Data Leakage, because no weakness in normal activities…
  - Average security support answer in regards of fail. What? Normal activities?
  - Guys, I can spend small amount of money ($$) to steal the user data with fake networks in public places!

WHAT COMPANIES THINK ABOUT 'QUOTES' AND INSECURITY

- In its defense, AgileBits insisted that AgileKeychain was still secure, and noted that the format dates back to 2008 when the company was concerned about speed and battery drain problems caused by encryption.
  - http://appleinsider.com/articles/15/10/20/1password-to-change-file-formats-after-key-file-found-to-contain-unencrypted-data
- If you browse to your .agilekeychain "file" on disk, you find that it is actually a directory. Inside this directory is a file named "1Password.html".
  - http://timedoctor.org/2015/10/misleading-headlines-popularity-rises-200/

[AGENDA]

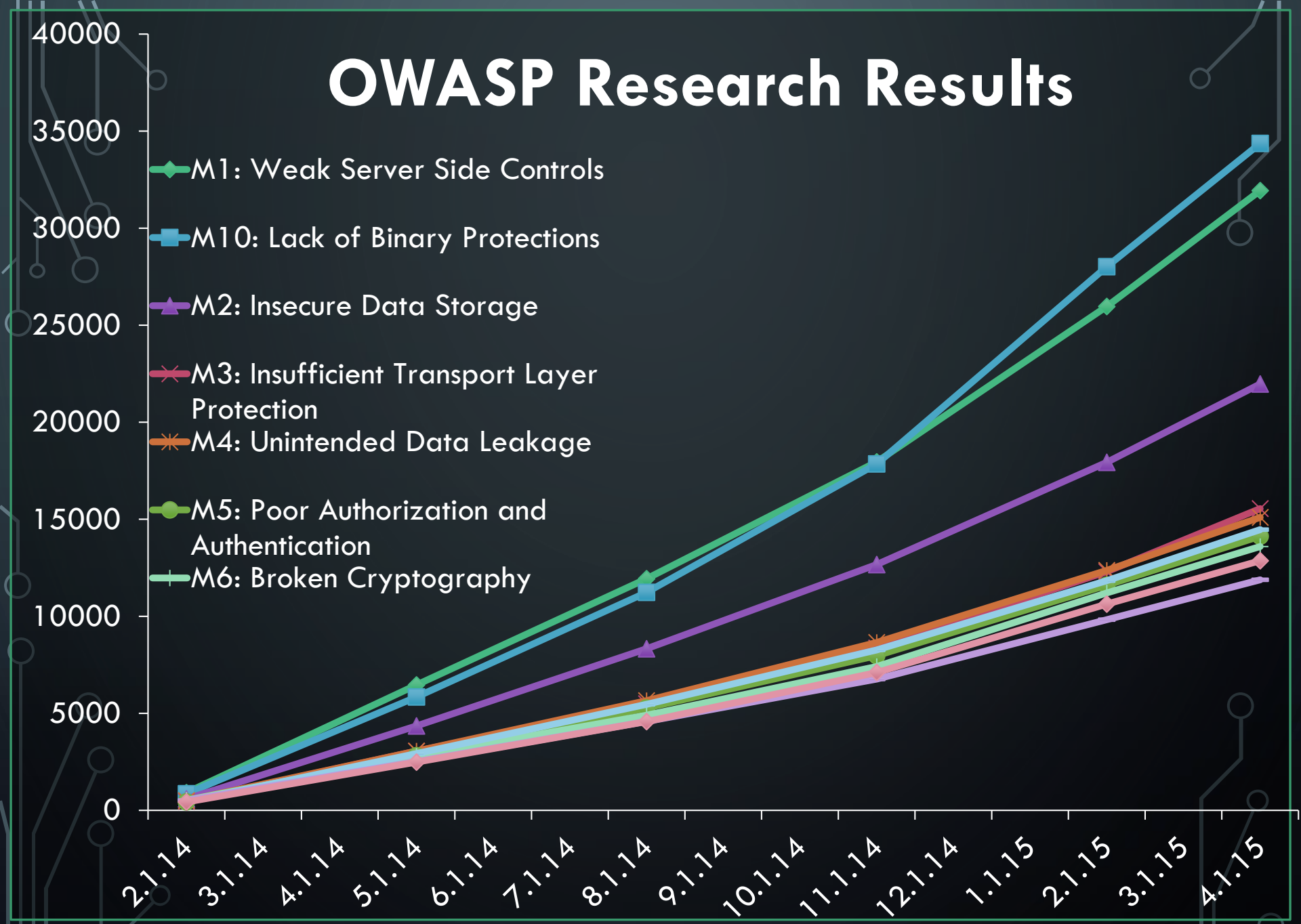
- ~~Intro~~

1. **First Part "What we already know about insecurity?"**
   - ~~InSecurity & InPrivacy Problem~~
   - ~~Poll~~
   - ~~Quotes about insecurity from researchers~~
   - ~~What companies think about 'quotes'~~
   - **Facts about app insecurity**
   - How can you make your app fail

OK, DEVELOPER, YOU'RE RIGHT. LET'S KNOW WHAT SURVEYS TELL US

- Data protection makes no sense, you're right, but …
- I'm not going to fall into examining many surveys.
- Just took couple of them
  - OWASP
  - ITR
- OWASP tells us that data leakage is kind growing issue
- ITR tells us there're 30% 'angry men' who want uninstall your app because privacy concerns

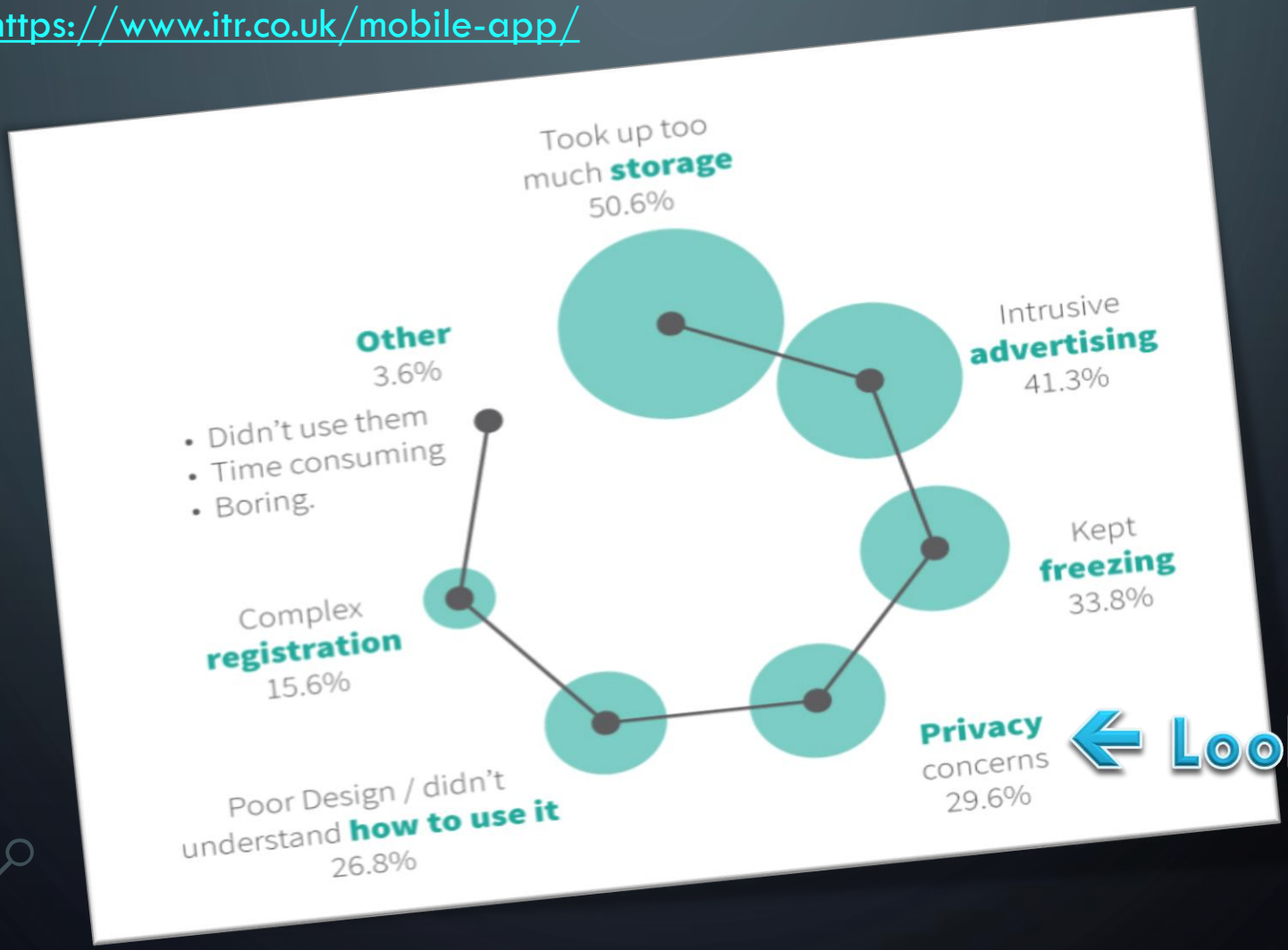
OWASP Research Results



https://www.owasp.org/images/9/9e/2015_Data_Synthesis_Results.pptx

ITR RESEARCH RESULTS.
WHY CONSUMER UNINSTALLED MOBILE APPS

https://www.itr.co.uk/mobile-app/



FACTS ABOUT APP INSECURITY

- Researchers find data leaks in Instagram, Grindr, OoVoo and more. The problems include storing images and videos in unencrypted form on Web sites, storing chat logs in plaintext on the device, sending passwords in plaintext…
  - http://www.cnet.com/news/researchers-find-data-leaks-in-instagram-grindr-oovoo-and-more

- Another Popular Android Application, Another Leak. We have found that another popular Google play app, “Camera360 Ultimate,” not only enhances the users’ photos but also inadvertently leaks sensitive data, which gives malicious parties unauthorized access to users’ Camera360 Cloud accounts and photos.
  - https://www.fireeye.com/blog/threat-research/2015/08/another_popular_andr.html

FACTS ABOUT APP INSECURITY

- At first glance, the VK Music app only displayed legitimate functionality – it played audio files uploaded to the social network. But further study showed that it also contained malicious code designed to steal VKontakte user accounts and promote certain groups on the social network.
  - https://securelist.com/blog/incidents/72458/stealing-to-the-sound-of-music/

- "In Russia will be kept of phone numbers, logins and passwords of users. Messages we do not store, they are on the devices of users," Moscow representative of the company Viber said. According to the company's lawyers, messengers also fall under the law which requires to store personal data of Russians on servers located on the territory of the country.
  - http://appleapple.top/viber-moved-their-servers-to-russia/

FACTS ABOUT APP INSECURITY

- InstaAgent, an app that connects to Instagram and promises to track the people that have visited a user's Instagram account, appears to be storing the usernames and passwords of Instagram users, sending them to a suspicious remote server.
- An app developer from Peppersoft downloaded InstaAgent -- full name "Who Viewed Your Profile - InstaAgent" -- and discovered it's reading Instagram account usernames and passwords, sending them via clear text to a remote server - instagram.zunamedia.com.
- http://www.macrumors.com/2015/11/10/malicious-instaagent-instagram-app/

FACTS ABOUT APP INSECURITY

- Russian's largest travel search engine, Aviasales (known worldwide as JetRadar), enriched its mobile application with the ability to capture and submit all necessary passenger's data in a few clicks. The application offers customer to make a picture of Machine-Readable Zone (MRZ) of his/her passport and uses ABBYY Cloud OCR Engine to extract data from the picture. Once the MRZ was recognized all the user need is to verify the captured data before saving it for future purchases or applying it to the current one. Learn more from the Case Study.
  - http://ocrsdk.com/customers/
  - http://www.abbyy.com/casestudies/one-click-between-you-and-your-perfect-holidays/#sthash.B4vyhtCD.M1ntvmDJ.dpbs
- They take screenshot, recognize the passport and do you really think they protect your data ? ☺

[AGENDA]

- ~~Intro~~

1. **First Part "What we already know about insecurity?"**
   - ~~InSecurity & InPrivacy Problem~~
   - ~~Poll~~
   - ~~Quotes about insecurity from researchers~~
   - ~~What companies think about 'quotes'~~
   - ~~Facts about app insecurity~~
   - **How can you make your app fail**

HOW CAN YOU MAKE YOUR APP FAILS

- **Forget about boundaries – WhatsApp and other apps**
  - ✓ Detect public or external storage folders
  - ✓ Put almost of all data into them!
  - ✓ Ask user, use it for backup, store only extra large files
- **Ignore security at all – almost each payment app**
  - ✓ Ask for payment credentials
  - ✓ Let everyone MITM it
  - ✓ Ask for it but find a way to transfer secure to server, perform a payment and get back to user with result
- **Don't care about each OS or platform – Vkontakte, etc.**
  - ✓ Release apps per each OS and Platform
  - ✓ Fix a security holes in one or two apps
  - ✓ Stop doing that

HOW CAN YOU MAKE YOUR APP FAILS

- **Assure everyone you never fail - 1Password and other apps**
  - ✓ Say, we care only vulnerabilities. Data leakage? Don't install viruses or jailbreak yourself!
  - ✓ You need no protection! It speeds our app up!
  - ✓ Stop that madness
- **Make it useless Shy Russian Bank App ☺**
  - ✓ Implement root detection
  - ✓ Believe no one will ever patch your app having rooted device
  - ✓ Understand useless of you security controls in case non-rooted and rooted devices
- **Believe in power of 3rd party security addons - Shy Russian AV Seller ☺**
  - ✓ Buy, sell, implement AV-addon
  - ✓ Make it not runnable on many devices & believe no one would turn it off
  - ✓ Keep buying, selling, implementing

[AGENDA]

- ~~Intro~~
- ~~First Part "What we already know about insecurity?"~~
- **Second part "What are we going to know?"**
  - **Previous Research**
  - Research limits
  - Default security controls in different OS and its limits
  - Average Results by data category, app category, and protection type
  - Pretty interesting security and privacy fails

PREVIOUS RESEARCH

- I did many researches on mobile and app security.
- First of them were about something average between OS and Apps – BlackBerry, Android
- It was published and present around the world
- New Research
  - Included ~200 apps, for Cross OS apps provide - *protection concepts, OS specifics per concept, outlines & remediation, EMM specifics*
  - Was doing 2013 - 2014 and some event to show results.
  - "We know Twitter & Dropbox are better secured than bank apps!"
  - http://www.slideshare.net/EC-Council/hh-yury-chemerkin
  - http://defcamp.ro/dc14/Yury_Chemerkin.pdf
- Current Research ~700 apps
- + Bonus – Security & Privacy Project (demo, atm)

[AGENDA]

- ~~Intro~~
- ~~First Part "What we already know about insecurity?"~~
- **Second part "What are we going to know?"**
  - ~~Previous Research~~
  - **Research limits**
  - Default security controls in different OS and its limits
  - Average Results by data category, app category, and protection type
  - Pretty interesting security and privacy fails

RESEARCH LIMITS

- Researched cross-platform apps updated prior one month before event, but may
  - not available or pretend to the latest version due to countries restrictions
  - not available for all platforms because it wasn't released
  - not refer to analytics sdk like flurry or similar
- Any app data presented here do in plaintext (incl. easy bypassing)
  - Store data even in public/shared folders or on external drives
    - iOS < 8.3 has less local data protection controls and you can get access to them w/o jailbreak
  - Store in memory as is at least one time
  - Store in keychain on iOS and it's not additionally encrypted
  - Transferred via https or http without any additional protection and may be under simple MITM attack except
    - some native services of iOS, BlackBerry, Google & Windows Markets
    - most of all native Apps (BlackBerry, Win Modern 10 Apps) and a few 3rd party like Dropbox

[AGENDA]

- ~~Intro~~
- ~~First Part "What we already know about insecurity?"~~
- **Second part "What are we going to know?"**
  - ~~Previous Research~~
  - ~~Research limits~~
  - **Default security controls in different OS and its limits**
  - Average Results by data category, app category, and protection type
  - Pretty interesting security and privacy fails

DATA ACCESS PROTECTION IN OS

	Android	Mac OS	iOS OS	Windows OS	Windows Modern OS	Windows Mobile OS	BlackBerry OS
In-Rest	Need root, except public folders	No need root or jailbreak	Need jailbreak for keychain only (iOS < 8.3) Need jailbreak except public folders (iOS >=8.3)	No need root or jailbreak	Need Owner & Permissions Reassign	No tool for root or jailbreak	Backup access No tool for root or jailbreak Data maybe stored in public folders
In-Use	Need root	No need root or jailbreak	Need jailbreak	No need root or jailbreak	No need root or jailbreak	No tool for root or jailbreak	No tool for root or jailbreak
In-Transit	Need certificate, Optional proxy tool	Need certificate, +proxy tool	Proxy tool only (rarely) Need certificate, +proxy tool	Need certificate, +proxy tool	Need certificate, +proxy tool	MITM isn't allowed, passive http sniffing	MITM isn't allowed, passive http sniffing

[AGENDA]

- ~~Intro~~
- ~~First Part "What we already know about insecurity?"~~
- **Second part "What are we going to know?"**
  - ~~Previous Research~~
  - ~~Research limits~~
  - ~~Default security controls in different OS and its limits~~
  - **Average Results by data category, app category, and protection type**
  - Pretty interesting security and privacy fails

DATA TYPE (CATEGORIES)

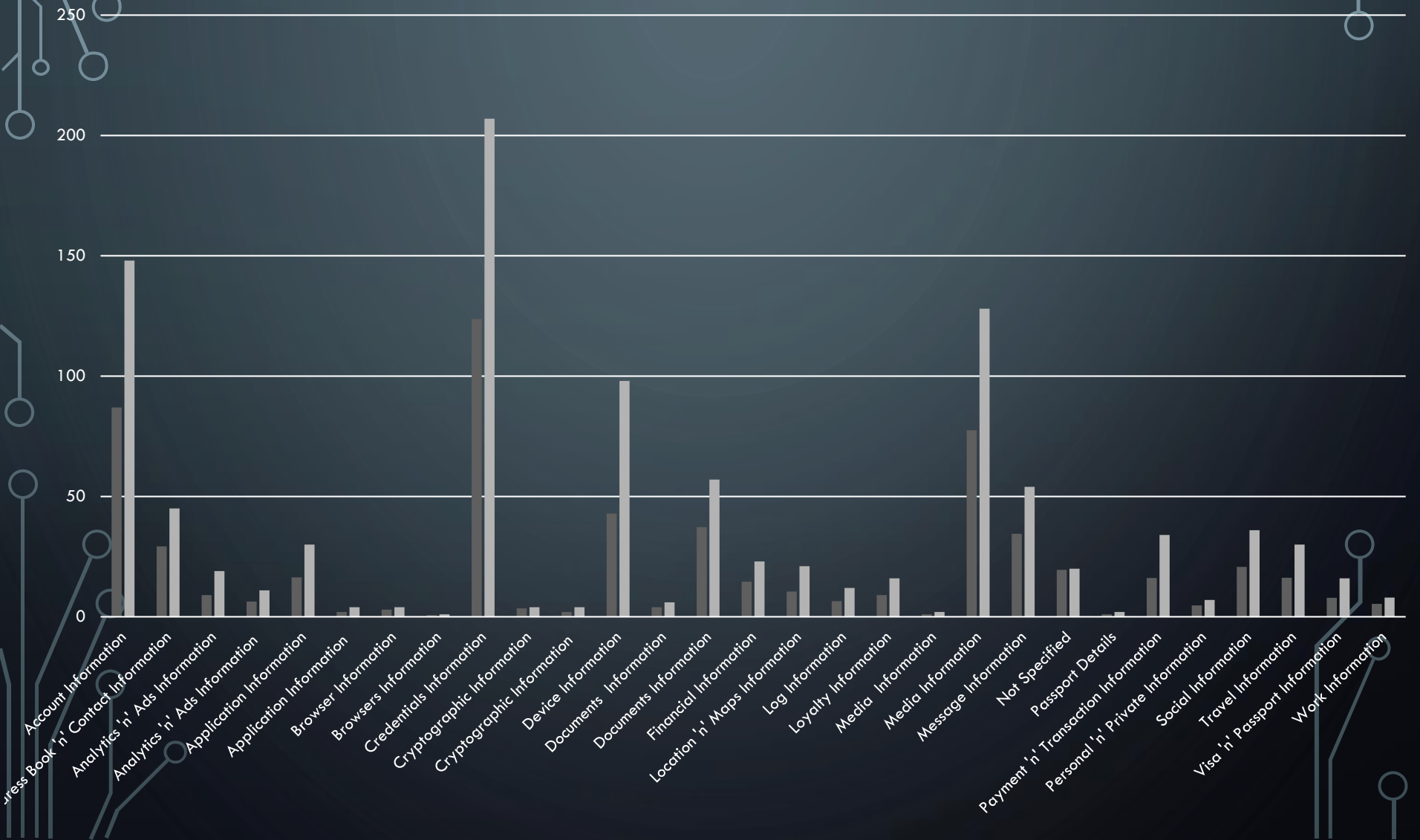
- Account Information
- Address Book 'n' Contact Information
- Application Information
- Booking Information
- Browser Information
- Call Information
- Credentials Information
- Cryptographic Information
- Device Information
- Documents Information
- Events Information
- Financial Information
- Location 'n' Maps Information
- Log Information
- Loyalty Information
- Media Information
- Message Information
- Personal 'n' Private Information
- Payment 'n' Transaction Information
- Social Information
- Tax 'n' Driver Information
- Travel Information
- Work Information
- Visa 'n' Passport Information

DATA PROTECTION SCORE

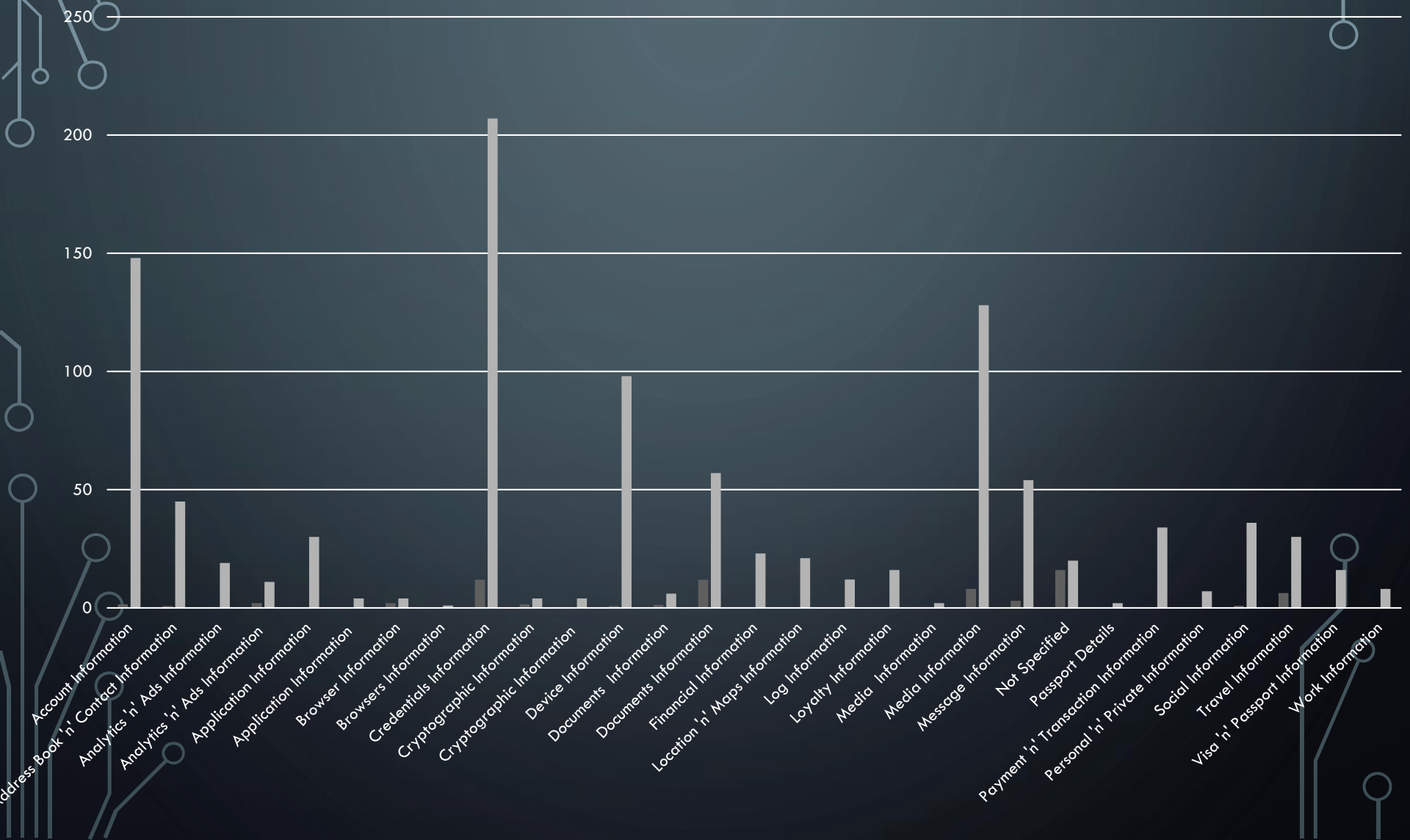
- There're 3 data protection concepts at least
  - Data-At-Rest
  - Data-In-Use
  - Data-in-Transit
  - …
- There're 2 type of protection
  - System protection (sandbox, ssl, etc.)
  - Own protection (encryption, access management, etc.)

- There're several level of protection per each type
  1. Non-Protected
  2. Compressed
  3. Weak Protected
  4. Extra
  5. Medium Protected
  6. Cached
  7. Protected
  8. Strong Protected
  9. Not Specified

ABOUT 700 APPS WERE EXAMINED. SYSTEM CONTROLS



ABOUT 700 APPS WERE EXAMINED. OWN DEVELOPED CONTROLS



MOST SECURED APP. DATA-IN-TRANSIT

[SYSTEM] STRONG PROTECTED | NON-PROTECTED [OWN]

iOS / Android	British Airways	Payment 'n' Transaction Information
iOS / Android	Dropbox	Not Specified
iOS / Android	eFax	Message Information
Android	Instagram	Account Information, Credentials Information
Android	Instagram	Address Book 'n' Contact Information
Android	Sberbank	Address Book 'n' Contact Information
Android	Sberbank	Account Information, Credentials Information
Android	Sberbank	Work Information
Android	Sberbank	Visa 'n' Passport Information
Android	Sberbank	Application Information
Android	Sberbank	Device Information, Financial Information
Android	Sberbank	Payment 'n' Transaction Information
iOS / Android	VTB24	Not Specified
iOS / Android	Kik	Messages, Credentials (Passwords)
iOS / Android	AirBnb	Card Short Information
iOS / Android	Amazon Cloud Drive	Sync Documents
iOS / Android	Amazon Photos	Sync Documents

MOST SECURED APP. DATA-IN-TRANSIT

[SYSTEM] ANY PROTECTED | STRONG OR PROTECTED [OWN]

Android	4talk	Network
Windows Desktop	4talk	Network
iOS/iPhone	QIWI	Credentials Information + Any Data
iOS/iPad	QIWI	Credentials Information + Any Data
Android	QIWI	Credentials Information + Any Data
iOS/Android	RSB	Credentials Information (Tokens = hash of passw)
iOS/Android	Twitter	Credentials Information
iOS/Android	Twitter	Social Information
iOS/Android	Viber	Device Information, Account Information
iOS/Android	Viber	Message Information, Media Information
iOS/Android	WhatsApp	Cryptographic Information
iOS/Android	WhatsApp	Message Information
iOS/Android	WhatsApp	Media Information
Android	ColorNote	Calendar Details, Calendar Events, Notes
iOS/Android	Hangouts	Messages

MOST SECURED APP. DATA-AT-REST

[SYSTEM] ANY PROTECTED | STRONG OR PROTECTED [OWN]

Android	4talk	vCard
Windows Desktop	4talk	Local storage (any data)
iOS/Android	Anews	Credentials (Tokens)
iOS	British Airways	Credentials (Tokens)
iOS	Delta Fly	Credentials (IDs), Credentials (Passwords)
iOS/Android	Dolphin	Credentials (Passwords)
iOS	Evernote	Credentials (Tokens)
iOS	KLM	Credentials (Passwords)
iOS/Android	Maxthon	Credentials (Passwords)
iOS/Android	RSB	Credentials Information (Tokens = hash of passw)
iOS/Android	WhatsApp	Credentials (Passwords), Encryption key

MOST SECURED APP. DATA-AT-REST. IOS :: PROTECTED SNAPSHOTS [OWN]

iOS	Citi Mobile	Media Information (Screen Snapshots)
iOS	DocToGo	Media Information (Screen Snapshots)
iOS	Google Drive	Media Information (Screen Snapshots)
iOS	OneDrive Business	Media Information (Screen Snapshots)
iOS/iPhone	QIWI	Media Information (Screen Snapshots)

MOST SECURED APP.

[SYSTEM] ANY PROTECTION | CACHED [OWN]

iOS/Android IHG	Orders & Reservation Details, Orders & Reservation History
iOS/Android Delta	Orders & Reservation Details, Orders & Reservation History
iOS/Android British Airways	Orders & Reservation Details, Orders & Reservation History
iOS/Android Yandex Drive	Media Data, Documents or synchronized data
iOS/Android OneDrive	Media Data, Documents or synchronized data
iOS/Android OneDrive Business	Media Data, Documents or synchronized data
iOS/Android MS Office apps	Media Data, Documents or synchronized data
iOS/Android Google Photos	Media Data, Documents or synchronized data
iOS/Android Adobe	Media Data, Documents or synchronized data
iOS/Android Dropbox	Media Data, Documents or synchronized data
iOS/Android Maxthon	Cached viewed pages and synchronized data
iOS/Android Blogger	Cached viewed pages and synchronized data

MOST SECURED APP. MAC OS X APPS

[SYSTEM] STRONG OR PROTECTED | NON-PROTECTED [OWN]

Mac OS X	4talk	Credentials Info - Password (in keychain)
Mac OS X	Viber	Device, Account, Message Information
Mac OS X	Yandex Drive	Media, Device, Account, Documents Information
Mac OS X	Dropbox	Media, Device, Account, Credentials, Documents Information
Mac OS X	Mail.RU Cloud	Media, Device, Account, Credentials, Documents Information
Mac OS X	ICQ	Credentials Info - Password (in keychain)
Mac OS X	OneDrive	Credentials Info - Token (in keychain)
Mac OS X	Google Drive	Credentials Info - Token (in keychain)
Mac OS X	Evernote	Credentials Info - Password (in keychain) = md5 hash value
Mac OS X	Amazon Cloud Drive	Credentials Info - Token (in keychain)
Mac OS X	Box	Credentials Info - Token (in keychain)
Mac OS X	MS Outlook	Credentials Info - Token (in keychain)

MOST SECURED APP. WIN MOBILE 10

[SYSTEM] STRONG / PROTECTED BY DEFAULT | NON-PROTECTED [OWN]

Project Astoria is delayed
http://www.windowscentral.com/microsofts-project-astoria-delayed

Win Mobile 10	All apps mentioned in presentation	Store everything in plaintext at Rest (locally)
Win Mobile 10	All apps mentioned in presentation	Have a system protected network layer by OS by default from MITM attacks according to the June developer's preview build

MOST SECURED APP. BLACKBERRY 10

[SYSTEM] STRONG / PROTECTED BY DEFAULT | NON-PROTECTED [OWN]

BlackBerry 10	All apps mentioned in presentation	Protected locally by OS by default but all data stored in plaintext and can be accessed via app data backups. Work for BlackBerry & Android apps
BlackBerry 10	All apps mentioned in presentation	Have a network layer protected by OS by default but http data can be stolen Work for BlackBerry & Android apps

SPECIAL PART FOR DEFCAMP 2016. LAST MINUTE RESEARCH

- Everyone got a booklet-guide. Here was a short info about trusted taxi companies.

- Meridian – no in-app payment features, store & transmitting everything in plaintext
  - Account, Local'n'Maps, and Device Information

- SpeedTaxi – no in-app payment features, store & transmitting everything in plaintext. Some issues with a server
  - Account, Local'n'Maps, Device and Message Information

- Cobalcescu – no in-app payment features, store & transmitting everything in plaintext. Some issues with a server
  - Account and Travel Information

APPS. OUTLINES

- Let's summarize our findings about
  - IM apps
  - Travels apps
  - Office apps
  - Bank apps
  - Payments apps
  - Social apps

IM APPS. TYPICAL BEHAVIOR

- Storing data (conversations) in plaintext locally
- Transmitting data via https without protection from MITM & trusted certificate to sniff the traffic
  - Some apps don't use http(-s) at least
- Storing credentials in plaintext, usually token instead of password
- Transmitting credentials in plaintext first, rest of time token instead of password
- Keep social tokens without any protection

TRAVEL APPS. TYPICAL BEHAVIOR

- Storing data in plaintext locally
  - Some apps have a reduced history limited by 30-180 days
- Transmitting data via https or even http without protection from MITM & trusted certificate to sniff the traffic
  - Some apps have a reduced history limited by 30-180 days
- Storing credentials in plaintext, sometimes token instead of password
- Transmitting credentials in plaintext first, sometimes token instead of password

OFFICE/BUSINESS APPS. TYPICAL BEHAVIOR

- Storing data in plaintext locally
  - Some apps store it in hidden folders, as a separated cached files
- Transmitting data via https without protection from MITM & trusted certificate to sniff the traffic
  - Some apps prevent MITM running under random OS
- Storing credentials in plaintext, sometimes token instead of password
- Transmitting credentials in plaintext first, sometimes token instead of password

BANK APPS. TYPICAL BEHAVIOR

- Rarely storing anything locally but do it in plaintext
  - Some apps store cached data, it's hard to catch it
- Transmitting data via https without protection from MITM & trusted certificate to sniff the traffic
  - A few apps prevent MITM
- Storing credentials in plaintext, sometimes token instead of password
- Transmitting credentials in plaintext first, sometimes token instead of password

PAYMENTS APPS. TYPICAL BEHAVIOR

- Storing data in plaintext locally
- Transmitting data via https without protection from MITM & trusted certificate to sniff the traffic
  - Some apps prevent MITM and have its own cryptography
- Storing credentials in plaintext, usually token instead of password
- Transmitting credentials in plaintext first, rest of time token instead of password

SOCIAL APPS. TYPICAL BEHAVIOR

- Storing data in plaintext locally
- Transmitting data via https without protection from MITM & trusted certificate to sniff the traffic
- Storing credentials in plaintext, password or token still gives full access
- Transmitting credentials in plaintext first, password or token still gives full access

[AGENDA]

- ~~Intro~~
- ~~First Part "What we already know about insecurity?"~~
- **Second part "What are we going to know?"**
  - ~~Previous Research~~
  - ~~Research limits~~
  - ~~Default security controls in different OS and its limits~~
  - ~~Average Results by data category, app category, and protection type~~
  - **Pretty interesting security and privacy fails**

PRETTY INTERESTING SECURITY AND PRIVACY FAILS

- Whatsapp encrypts backup with certain key but

  - never encrypts non-backed up (locally stored) data …. the same data (!)
- Whatsapp users exchange their messages & media. It stored in plaintext on Whatsapps servers. At least it requested in plaintext
  - We found audio notes URLs
    - https://mmv326.whatsapp.net/d/ny……X7.mp3
  - We found photo URLs
    - https://mmi621.whatsapp.net/d/7m……..Bt.jpg
- Also we found an interesting command to turn off encryption between 2 whatsapp app. It works for Android but iOS reject it ☺
  - http://m.heise.de/ct/artikel/Keeping-Tabs-on-WhatsApp-s-Encryption-2630361.html

PRETTY INTERESTING SECURITY AND PRIVACY FAILS HOW TO FAIL WITH HTTPS

- Be any app like [AirCanada] and send information about device and environment
- Be news/social app like [Anews/Flipboard] and send everything in plaintext via http
- Be storage app like [Asus WebStorage] and send credentials in plaintext
  - (also fail with old hash algorithm, see next slides)
- Be travel app like [AviaSales / Momondo], send everything in plaintext and rely on 3rd party server MITM protection
- Be storage app like [Box], prevent MITM but fail and reveal credentials to MITM tool
- Be taxi app like [Gett / MaximTaxi] and send everything in plaintext, also fail with MITM protect of my credit card
- Be hotel app like [Hotels.ru] and fail everywhere even with sending a password in mail body in plaintext

PRETTY INTERESTING SECURITY AND PRIVACY FAILS THE WEAKEST APP UNDER CERTAIN OS (!)

- Asus WebStorage
  - Make users type their password in different cases (upper & lowercase)
  - Instead, Asus app takes the MD5 hash value of lowercased password

- Hangouts (former Gtalk)
  - Incoming messages are encrypted additionally
  - Outcoming messages are in plaintext
  - …still researching this app to find out «why?»

- Amazon CloudDrive
  - Prevent you from MITM attacks and accessing the Amazon server
  - …but reveals password for proxy tool

- Amazon Photos
  - Prevent you from MITM attacks and accessing the Amazon server
  - …but reveals password for proxy tool

PRETTY INTERESTING SECURITY AND PRIVACY FAILS THE WEAKEST APP UNDER CERTAIN OS (!)

- 4talk
  - Y2014 wasn't protected at all
  - Y2015: Protected for Windows at-rest & transit, prevents MITM
  - Y2015: Protected for Android in-transit only (no MITM), no local protection
  - Y2015: still not protected for iOS and Mac OS at all

- App-in-the-Air
  - Android app & iOS iPhone only app. Network is medium protected (https).
  - MITM is possible, needs trusted certificate
  - ~~iOS iPad only app. Everything goes in http without any protection~~
    - Fixed (!) Now, no difference between iPhone and iPad apps. Update: Nov 3-4th

- Vkontakte
  - Android app & iOS iPhone only app. Network is medium protected (https).
  - MITM is possible, needs trusted certificate
  - iOS iPad only app. Network is weak protected (https). MITM is possible, no needs trusted certificate.

PRETTY INTERESTING SECURITY AND PRIVACY FAILS
THE WEAKEST APP AMONG OTHERS NO IN REGARDS ANY OS

- Weak Protection in-Transit. MITM is possible without trusted fake certificate (!)

- Aeroexpress – good app to buy a ticket for a train to the airport

- AnyWayAnyDay – in 2013 they had 2x‘anywayanyday’ (192 bit) hardcoded. I told on conference about it. Now, in 2015 it goes more secure – 3x ‘anywayanyday’ (256 bit).

- British Airways – failed everywhere except booking tickets. Here we failed with cert even

- eFax – except downloading faxes. We got URL to download but faxes didn’t download. Here MITM failed with cert even.

- Platius – this payment app was bought by Russian Bank

- RocketBank – this payment app was bought by another one

OUTLINES & REMEDIATIONS

OUTLINES: ANDROID

- Credentials stored or transferred in plaintext locally.
- OS does not provide any protection like a keychain in iOS
- Data usually stored or transferred structured file type that simplify an analysis
- Signature-based encryption that helps to quickly decrypt data (depends on dynamically linked libraries)
- Data stored in SQLite databases usually not encrypted
- Data stored on external memory (SD card) rarely encrypted
- Keys may be hardcoded or put in data folder

OUTLINES: IOS

- Credentials stored/ transferred in plaintext locally.
- Data stored in a keychain without additional protection or encryption
- Data usually stored or transferred structured file type that simplify an analysis
- Signature-based encryption that helps to quickly decrypt data
- Avoiding protection mechanism in iOS that leads to pure protection eventually
- Data stored in SQLite databases usually not encrypted
- iOS version <8.3
  - Application data can be accessed without jailbreak
- iOS version >=8.4 incl. 9.0.2
  - Application data can be accessed with jailbreak only
- Keys may be hardcoded

OUTLINES: BLACKBERRY

- BlackBerry Apps & Services prevent transferring data via untrusted connection even
- System protection storage couldn't be easily access
- Apps usually store data in shared folders (docs, audio, etc.) are available to read/write for all
- Quite difficult to make BlackBerry trust to the proxy-certificates
- Android apps running on BlackBerry don't differ from other Android apps neither network, nor local

OUTLINES: WINMOBILE 10

- Credentials stored or transferred in plaintext locally.
- Data usually stored or transferred structured file type that simplify an analysis
- Signature-based encryption helps quickly decrypt data (depends on dynamically linked libraries)
- Data stored in SQLite databases usually not encrypted
- Keys may be hardcoded or put in data folder
- Applications could be analyzed on Windows 10 Desktop via known methods like a desktop applications

OUTLINES: WIN 10

- Credentials stored or transferred in plaintext locally.
- Data usually stored or transferred structured file type that simplify an analysis
- Signature-based encryption helps quickly decrypt data (depends on dynamically linked libraries)
- Data stored in SQLite databases usually not encrypted
- Keys may be hardcoded or put in data folder
- Application data folder is access without any restrictions

OUTLINES: MAC OS X

- Credentials stored/ transferred in plaintext locally.
- Data stored in a keychain without additional protection or encryption
- Data usually stored or transferred structured file type that simplify an analysis
- Signature-based encryption that helps to quickly decrypt data
- Avoiding protection mechanism in iOS that leads to pure protection eventually
- Data stored in SQLite databases usually not encrypted
- Keys may be hardcoded
- Application data folder is access without any restrictions

REMEDIATION: ANDROID

- Follow security programming guide from Google
- Call ‘setStorageEncryption’ API for locally stored files (new Android OS v5+)
- Encrypt externally stored files on SD Card or Cloud (any OS)
- Define when encryption signature doesn’t matter, else avoid it
- Reduce using of ‘MODE_WORLD_READABLE ’ unless it really needs
- Avoid hardcoded and debug tracks as much as possible (it’s easy to decompile)
- Add extra protect beyond OS (encryption, wiping, etc.)

REMEDIATION : IOS

- Follow security programming guide from Apple
- Never store credentials on the phone file system. Use API or web scheme instead
- Define when encryption signature doesn't matter, else avoid it
- Use implemented protection mechanism in iOS…
- But … add extra protection layer beyond OS protection in case of jailbreak
- Use any API and protection mechanisms properly but never default settings
- Don't forget to encrypt SQL databases

REMEDIATION : BLACKBERRY

- Follow security programming guide from BlackBerry
- Don't store credentials in shared folders
- Encrypt data stored in shared folders
- Use implemented protection mechanism in BlackBerry…
- But … add extra protection layer beyond just in case
- Don't forget to encrypt SQL databases
- Don't develop Android app-ports
- Try to avoid using ported or Android native app under BlackBerry
- Develop more and use native apps for BlackBerry □

REMEDIATION: WINMOBILE 10

- Credentials stored or transferred in plaintext locally.
- Data usually stored or transferred structured file type that simplify an analysis
- Signature-based encryption helps quickly decrypt data (depends on dynamically linked libraries)
- Data stored in SQLite databases usually not encrypted
- Keys may be hardcoded or put in data folder
- Applications could be analyzed on Windows 10 Desktop via known methods like a desktop applications

REMEDIATION : WIN 10

- Credentials stored or transferred in plaintext locally.
- Data usually stored or transferred structured file type that simplify an analysis
- Signature-based encryption helps quickly decrypt data (depends on dynamically linked libraries)
- Data stored in SQLite databases usually not encrypted
- Keys may be hardcoded or put in data folder
- Application data folder is access without any restrictions

REMEDIATION : MAC OS X

- Credentials stored/ transferred in plaintext locally.
- Data stored in a keychain without additional protection or encryption
- Data usually stored or transferred structured file type that simplify an analysis
- Signature-based encryption that helps to quickly decrypt data
- Avoiding protection mechanism in iOS that leads to pure protection eventually
- Data stored in SQLite databases usually not encrypted
- Keys may be hardcoded
- Application data folder is access without any restrictions

ADVICES.
YOU'RE DEVELOPER? DON'T CARE ABOUT SECURITY/PRIVACY? THEN YOUR CHOICE IS …

- **BlackBerry.** Protects everything locally stored except public folders & external storage. Also it's hardly to MITM except plain http traffic. Even for Android (!)
- **Windows Modern 10 apps.** Anti-MITM protection on OS level by default (still researching it, also can't confirm it for Android app support – Project Astoria)
- **iOS. Ok.** Easy way to make user to install trusted fake certificate to MITM. Upgrade! Local app files on iOS < 8.3 could be accessed without jailbreak
- **Android. Fail.** Easy way to make user to install trusted fake certificate to MITM. Some vendors prevent unlocking bootloader without user interaction to avoid root without his asking. But some doesn't (!)
- **Windows Desktop. Fail.** Easy way to change access permissions. MITM depends on certain app only
- **Mac OS. Fail.** Easy way to access app files. MITM depends on certain app only

[AGENDA]

- ~~Intro~~
- ~~First Part "What we already know about insecurity?"~~
- ~~Second part "What are we going to know?"~~
- **Third Part "What we can do with that?"**
  - **Project**
  - Goal
  - Current state, Features and Limits

[DEMO] PROJECT - CRAPPSECURITY

- We [as security experts] know what data is protected and not protected despite of it's locally stored, transferred or hardcoded
- Also, we know two simple things
  - not only users publish their data
  - developers can't protect data
- At the same time we're customers, right?
  - I'm as a customer prefer and have a right to know where my smartphone shouldn't be connected to network or plugged PC/Mac.
  - Developers aren't going to tell me if they fail. Instead they're telling 'everything is OK but we're not responsible for anything'

[AGENDA]

- ~~Intro~~
- ~~First Part "What we already know about insecurity?"~~
- ~~Second part "What are we going to know?"~~
- **Third Part "What we can do with that?"**
  - ~~Project~~
  - **Goal**
  - Current state, Features and Limits

[DEMO] PROJECT – CRAPPSECURITY GOAL

- Goal is providing a solution that helps to keep everyone informed about app security fails.
- *Everyone* means
  - app users as well as app developers
  - you don't need to be expert to understand that how it affects you; you just know if it has required level of protected or not
  - community-solution and help
- Free to join! ☺

[DEMO] PROJECT – CRAPPSECURITY *WHAT IS IT …*

- Community of independent security experts who want to help in filling a database and keep it up-to-date
- Knowledge DB about app data protection like CVE/NVD
- It covers mobile and desktop apps published in App markets
- It is available for desktop & mobile OS and web
- Also it can be part of security awareness solution
- 'App Data' Use case management (home, work, public, trusted places, etc.)
- Social & Sharing features to keep friends informed
- App data tracking in real-time

[AGENDA]

- ~~Intro~~
- ~~First Part "What we already know about insecurity?"~~
- ~~Second part "What are we going to know?"~~
- **Third Part "What we can do with that?"**
  - ~~Project~~
  - ~~Goal~~
  - **Current state, Features and Limits**

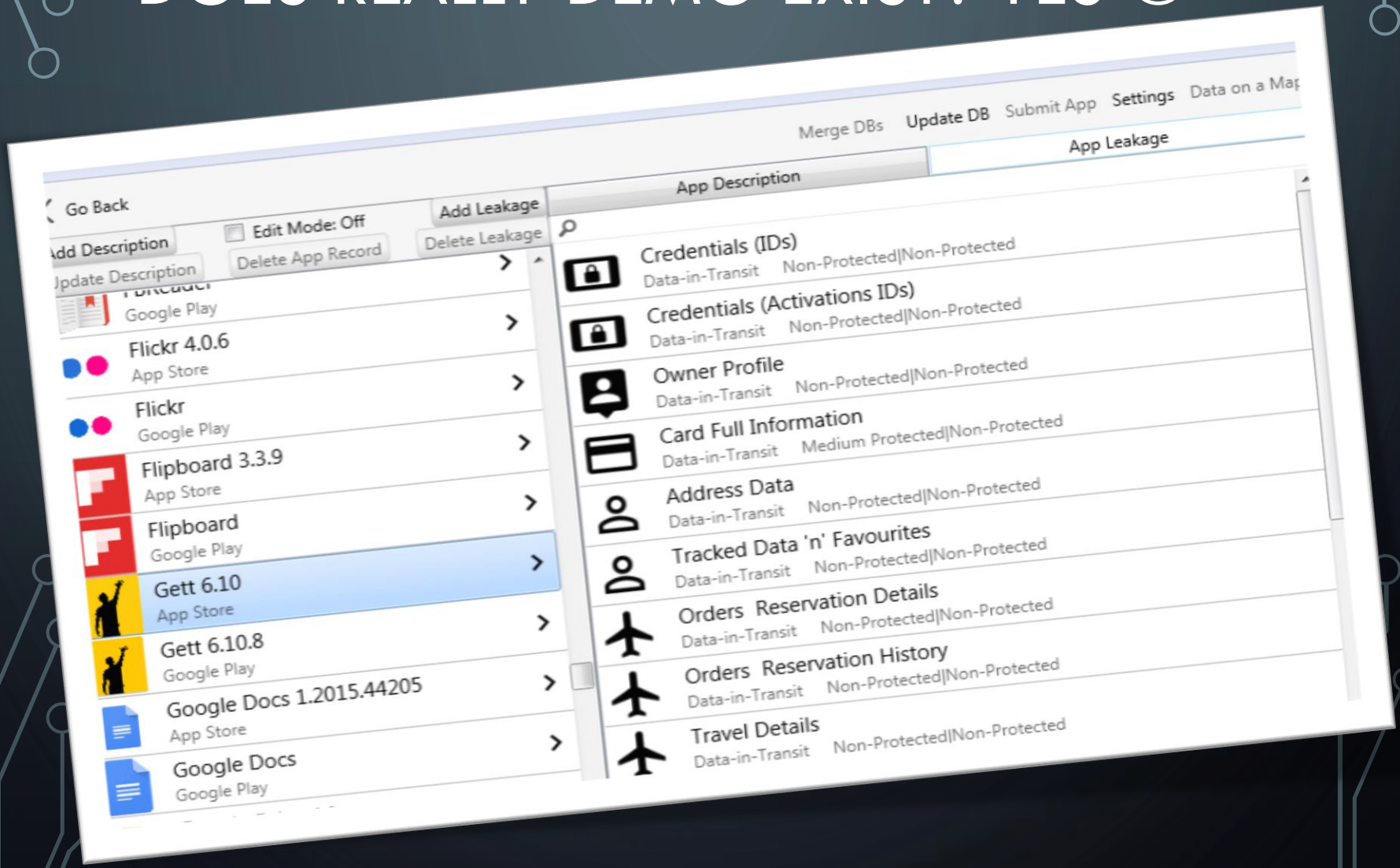
[DEMO] PROJECT – CRAPPSECURITY CURRENT STATE, FEATURES AND LIMITS

- How many apps we examined ?
  - 700+ including different OS, platforms and markets
- What limits?
  - Experts are limited by national scope of applicability per certain app
- OS supported
  - Desktop – Windows OS, Mac OS
  - Mobile – Android OS, iOS is upcoming
  - Android supported OS – BlackBerry, Windows Mobile 10 are upcoming
- When beta will be available – Spring, 2016
  - More apps, more data more security fails☺
  - Web site will store same information like desktop or mobile app tool
  - Channel for Devs, customers to fill our knowledge DB
- By now you can request a demo
  - for Desktop Windows & Mac OS and Android
  - limited by quantity of apps

[AGENDA]

- ~~Intro~~
- ~~First Part "What we already know about insecurity?"~~
- ~~Second part "What are we going to know?"~~
- ~~Third Part "What we can do with that?"~~
  - ~~Project~~
  - ~~Goal~~
  - ~~Current state, Features and Limits~~

[DEMO] PROJECT – CRAPPSECURITY DOES REALLY DEMO EXIST? YES ☺



SUMMARY

- Secured application isn't only application has no vulnerabilities of malware code but application that protects data in a right way and has no IAM & Crypto fails
- There is a few fragmented sources on data protection to handle it
  - You can find it in knowledge databases like CVE, CVSS, NVD or in articles, speeches, talks from time to time
- Only 2 Windows & BlackBerry protect application data without asking developer
- Rest OS (iOS, Mac OS, Android, Windows, Windows Modern) require application developer to manage it by himself
- If you know a bit more about how you app data protected, you could design 'app data' use cases to manage it properly depend on place you are (airport, public places, home, work, etc.)

POLL RESULTS

- Who wants to post his cats on Instagram only?
- Who wants to protect his application data instead?
- Who wants to protect customer data in his apps?
- Who believes that an absence of protection is speed boost feature

- Now, time to check the Poll results ☺

[YURY CHEMERKIN]

- MULTISKILLED SECURITY EXPERT
- WORK FOR ADVANCED MONITORING
- EXPERIENCED IN :
  - REVERSE ENGINEERING & AV, DEVELOPMENT (PAST)
  - MOBILE SECURITY, & CLOUD SECURITY
  - IAM, COMPLIANCE, FORENSICS
  - PARTICIPATION & SPEAKING AT MANY SECURITY CONFERENCES

UNTRUSTED MOBILE APPLICATIONS

STATE OF ART OF SECURITY APP-APOCALYPSE

YURY CHEMERKIN

SEND A MAIL TO: YURY.S@CHEMERKIN.COM

HOW TO CONTACT ME ?

ADD ME IN LINKEDIN:

HTTPS://WWW.LINKEDIN.COM/IN/YURYCHEMERKIN